

2131 #3



Attorney Docket No. 50325-0550

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Group Art Unit No.: 2131

Mihailo M. Stojancic, et al.

Examiner: NYA

Serial No.: 09/955,902

Filed on: September 18, 2001

For: PRE-COMPUTATION AND DUAL-PASS  
MODULAR ARITHMETIC OPERATION  
APPROACH TO IMPLEMENT ENCRYPTION  
PROTOCOLS EFFICIENTLY IN ELECTRONIC  
INTEGRATED CIRCUITS

RECEIVED  
DEC 21 2001  
Technology Center 2100

Commissioner for Patents  
Washington, D.C. 20231

INFORMATION DISCLOSURE STATEMENT

Sir:

Enclosed is a copy of Information Disclosure Citation Form PTO-1449 together with copies of the documents cited on that form. It is respectfully requested that the cited documents be considered and that the enclosed Information Disclosure Citation Form PTO-1449 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

Pursuant to 37 C.F.R. § 1.97, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability.

Pursuant to 37 C.F.R. § 1.97, this Information Disclosure Statement is being submitted under one of the following (as indicated by an "X" to the left of the appropriate paragraph):

- ☒ 37 C.F.R. §1.97(b).
- ☐ 37 C.F.R. §1.97(c). If so, then this Information Disclosure Statement includes one of the following:
  - ☐ A statement pursuant to 37 C.F.R. §1.97(e)

\_\_\_\_\_ 1.97(e)(1) The undersigned hereby states that each item of information contained in this information disclosure statement was first cited in communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this information disclosure statement.

\_\_\_\_\_ 1.97(e)(2) The undersigned hereby states that no item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in this information disclosure statement was known to any individual designated in §1.56(c) more than three months prior to the filing of this information disclosure statement.

\_\_\_\_\_ A check for \$180.00 for the fee under 37 C.F.R. § 1.17(p).

\_\_\_\_\_ 37 C.F.R. §1.97(d). If so, then this Information Disclosure Statement includes the following:

\_\_\_\_\_ A statement pursuant to 37 C.F.R. §1.97(e)

\_\_\_\_\_ 1.97(e)(1) The undersigned hereby states that each item of information contained in this information disclosure statement was first cited in communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this information disclosure statement; OR

\_\_\_\_\_ 1.97(e)(2) The undersigned hereby states that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in §1.56(c) more than three months prior to the filing of this information disclosure statement.

AND

\_\_\_\_\_ A check for \$180.00 for the fee under 37 C.F.R. §1.17(i) for submission of the Information Disclosure Statement.

\_\_\_\_\_ 37 C.F.R. §1.97(i). Wherein applicants are submitting references before the grant of a patent to be placed in the file but not considered by the Patent office.


- (1) Accordingly, copies of the references as listed on the attached Form PTO 1449 are submitted herewith for placement in the file. No certification or fees are deemed necessary.

Throughout the pendency of this application, please charge any additional fees, including any required extension of time fees, and credit all overpayments to deposit account 50-1302. A duplicate of this sheet is enclosed.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: December 5, 2001

  
Craig G. Holmes  
Reg. No. 44,770

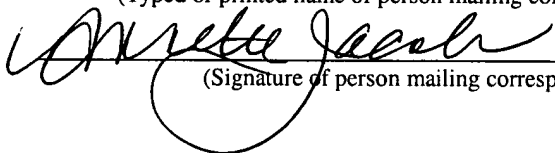
1600 Willow Street  
San Jose, California 95125-5106  
Telephone: (408) 414-1080  
Facsimile: (408) 414-1076

---

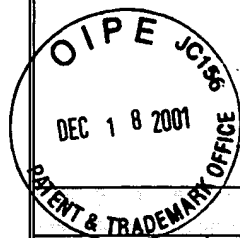
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, Washington, D. C. 20231 on December 6, 2001  
(Date of Deposit)

Annette Jacobs

(Typed or printed name of person mailing correspondence)

  
(Signature of person mailing correspondence)

**INFORMATION DISCLOSURE  
CITATION IN AN APPLICATION  
(PTO-1449)**



ATTY. DOCKET NO.  
**50325-0550**

SERIAL NO.  
**09/955,902**

APPLICANT  
**Mihailo M. Stojancic, et al.**

FILING DATE  
**September 18, 2001**

GROUP  
**2131**

**U.S. PATENT DOCUMENTS**

EXAMINER'S INITIALS	PATENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE

**FOREIGN PATENT DOCUMENTS**

EXAMINER'S INITIALS	PATENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
						Yes	No

**OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)**

	Cornell University, Computer Science Department, entitled "A Parallel Implementation of RSA", by David Pearson, dated July 22, 1996, (pgs. 1-10)
	IEEE Transactions on Computers, Vol. 47, No. 7, entitled "An RNS Montgomery Modular Multiplication Algorithm", by Jean-Claude Bajard, et al., © 1998 IEEE, dated July 1998, (pgs. 766-776)
	IEEE Transactions on Parallel and Distributed Systems, Vol. 6, No. 5, entitled "Modulo Reduction in Residue Number Systems", by Karl C. Posch, et al., © 1995 IEEE, dated May 1995, (pgs. 449-454)
	Swiss Federal Institute of Technology (ETH), Integrated Systems Laboratory, entitled "Efficient VLSI Implementation of Modulo $(2n \pm 1)$ Addition and Multiplication", by Reto Zimmerman, undated, (10 pgs.)
	RSA Laboratories, RSA Data Security, Inc., entitled "RSA Hardware Implementation", by Cetin Kaya Koc, Copyright © RSA Laboratories, Version 1.0, dated August 1995, (pgs. 1-28)
	Electrical & Computer Engineering, Oregon State University, entitled "A Scalable Architecture for Montgomery Multiplication", by Alexandre F. Tenca and Cetin K. Koc, undated, (15 pgs.)
	Proceedings of the 29 <sup>th</sup> Asilomar Conference on Signals, Systems and Computers, School of Electrical Engineering, University of Oklahoma, entitled "A Table-Lookup Scheme for Residue-to-Binary Conversion", by Chad C. Lamb and L.S. DeBrunner, © 1996 IEEE, (pgs. 214-217)
	TIMA Laboratory, entitled "Hardware for Computing Modular Multiplication Algorithm", by Alvaro Bernal and Alain Guyot, undated, (4 pgs)
	Dept. Electrical & Electronic Eng., University of Adelaide and Electronic Engineering Division, Cardiff University, entitled "Implementing 1,024-bit RSA Exponentiation on a 32-bit Processor Core", by B.J. Phillips and N. Burgess, © 2000 IEEE, (11 pgs)
	LIM-URA CNRS 1787, CMI, Universite de Provence, France and Dept. of Math and Computer Science, University of Odense, Denmark, entitled "An RNS Montgomery Modular Multiplication Algorithm", by Jean-Claude Bajard, et al., © 1997 IEEE, (pgs. 234-239)
EXAMINER	DATE CONSIDERED

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

**RECEIVED**  
**DEC 21 2001**  
Technology Center 2100

<b>INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)</b>				ATTY. DOCKET NO. <b>50325-0550</b>		SERIAL NO. <b>09/955,902</b>	
				APPLICANT <b>Mihailo M. Stojancic, et al.</b>			
				FILING DATE <b>September 18, 2001</b>		GROUP <b>2131</b>	
<b>U.S. PATENT DOCUMENTS</b>							
EXAMINER'S INITIALS	PATENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE	
<b>FOREIGN PATENT DOCUMENTS</b>							
EXAMINER'S INITIALS	PATENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
						Yes	No
<b>OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)</b>							
	LIRMM, Montpellier, France, Universite de Bretagne Occidentale, Brest, France, and SDU/Odense University, Denmark, entitled "Montgomery Modular Multiplication in Residue Arithmetic", by Jean-Claude Bajard, et al., dated November 1, 2000, (pgs. 1-11)						
	LIRMM, Montpellier, France, Universite de Bretagne Occidentale, Brest, France, and SDU/Odense University, Denmark, entitled "Modular Multiplication and Base Extensions in Residue Number Systems", by Jean-Claude Bajard, et al., undated, (7 pgs)						
	Digital Equipment Corp., Paris Research Laboratory (PRL), entitled "Fast Implementations of RSA Cryptography", by M. Shand, et al., undated, (9 pgs)						
	Thesis of Tolga Acar, Electrical & Computer Engineering, Oregon State University, entitled "High-Speed Algorithms & Architectures For Number-Theoretic Cryptosystems", by Tolga Acar, dated December 4, 1997 © by Tolga Acar 1997, (92 pgs)						
EXAMINER				DATE CONSIDERED			

**RECEIVED**  
 DEC 21 2001  
 Technology Center 2100

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.